Raneem Alarian
July 9, 2025

Case Analysis 2: An Ethics of Care Approach to Data Privacy Laws in the U.S.

In his article, "GDPR: An executive guide to what you need to know," Palmer describes the purpose, scope, and implications of the European Union's General Data Protection Regulation (GDPR). He details how the GDPR was enacted to provide individuals with more control over their personal data as a response to the increased misuse and mishandling of that data by organizations. Palmer points out that the regulation applies to any company processing the data of EU citizens, wherever the company is located. Central to the GDPR is the requirement for explicit user consent before data is collected, enabling users to access and erase their own personal information, and holding organizations accountable for the storage and use of that data. Companies are also required to report data breaches in a timely manner and are subject to serious penalties for non-compliance. The regulation demonstrates a firm commitment to protecting the privacy of individuals in an increasingly digital age. In this case analysis, I am going to argue that the ethics of care, together with Zimmerman and Buchanan's works, demonstrates that the United States should implement privacy laws similar to the GDPR because such laws emphasize our responsibility to prioritize user vulnerability, build relationships of trust, and highlight moral responsibilities toward people.

Zimmerman's Analysis Using Ethics of Care

Michael Zimmerman's work addresses the ethical issues that researchers and organizations encounter when they use data from online sites such as Facebook. Zimmerman argues against the frequent defense that public data is "fair game" for collection and analysis, pointing out that the context in which the data was shared often matters more than its technical accessibility. One of Zimmerman's key points is the notion of contextual integrity, which highlights the concept that just because information is publicly available does not mean it was intended for use in any conceivable context. When researchers or businesses use personal data outside of its intended context, they are violating the expectations and trust of the individuals who made it available. From an ethics of care perspective, contextual integrity is even more crucial. Ethics of care prioritizes empathy, mutual respect, and the care obligations we have towards others, particularly where one has more power than the other in the relationship. Online, for instance, data analysts and companies are more powerful than users who may not even know how their data is being used or commercialized. The ethics of care challenges the opinion of "data is public, therefore usable," and instead asks: are we being respectful of the human being behind the data? Are we preserving trust and care in this encounter?

Zimmerman's concerns over public data misuse have a direct connection to Palmer's explanation of GDPR. GDPR strives to reinstate a degree of control and care to data subjects by insisting on transparency, consent, and purpose limitation. Within the ethics of care, this matches the proposition that relationships, whether those between platforms and users, or governments and

citizens, need to be built on a basis of mutual respect, informed communication, and protection of vulnerability. Whenever companies extract data without actual consent or clear communication, they harm those relationships and address people not as persons, but rather as data points, disregarding the care and moral obligation due to them. Zimmerman's work also points out the long-term damage that can occur from ignoring these ethical responsibilities. Data, even if "public," can be reused in ways that damage people's reputations, safety, or autonomy. For instance, Facebook users might share personal information with their social network, never envisioning it will be scraped for research or marketed to third parties. Ethics of care reminds us that overlooking the emotional and relational aspects of data sharing can lead to genuine psychological or social harm, particularly for marginalized or less technologically literate people, who are more susceptible to abuse and less capable of speaking up for themselves.

In this context, the United States' current fragmented and inconsistent privacy policies come up short. In contrast to GDPR, which puts the burden of care on the organizations handling data, U.S. policy tends to put that burden on the user, assuming that they will read and comprehend a company's lengthy and complicated terms of service and take the initiative to opt out of intrusive online practices. Ethics of care disputes this individualistic thinking and favors a model in which those in power have an obligation to foresee harm, avert misuse, and uphold respectful and protective relationships with the individuals whose data they gather. Therefore, the ethics of care supports the application of GDPR-like protections in the United States. It is not merely a matter of legality or efficiency, it is a matter of creating a digital ecosystem in which users are treated with dignity, their expectations are respected, and their vulnerabilities are protected. Ethics of care demands a change in perspective from viewing users as passive sources of data to regarding them as human beings entitled to moral consideration and trust. The GDPR's foundational principles, such as clear consent, data minimization, and the right to be forgotten, demonstrate this moral attitude, and U.S. policy should follow that lead.

Buchanan's Analysis Using Ethics of Care

Buchanan's work discusses the nuanced ethical issues surrounding large-scale data collection from social media sites, particularly in the midst of politically or socially sensitive events. She looks at how researchers, law enforcement agencies, and other entities commonly defend scraping data from sites like Twitter since the data is technically publically available. Yet, Buchanan argues that relying on the "public" nature of data to defend its unlimited use overlooks the ethical aspects of context, power, and potential for harm, especially when users have no idea their data is being collected or analyzed in the first place. One of Buchanan's main ideas is the requirement for developing ethical frameworks that respond to the shifting nature of technology and data utilization. She describes how traditional informed consent models might not be adequate for big data settings, where people frequently contribute to datasets without realizing it and being excluded from discussions about how their information will be used. The ethics of care

is particularly applicable here since it compels researchers and institutions to be attentive to the relationship and power dynamics that are generally unseen in large-scale data practices. Just because people are not actively part of a research study or explicitly harmed doesn't mean they shouldn't be taken into account or protected.

In Buchanan's Twitter case study, people were tweeting about sensitive issues surrounding ISIS without knowing those tweets would later be collected, analyzed, and used for surveillance or political purposes. Ethics of care would criticize this method, not just for the absence of informed consent but also for the failure to honor the vulnerability of the people involved. Even if researchers mean well, ethics of care would require them to think about how their methodology impacts actual human beings. Are they protecting users and establishing trust? Do they know how their research can expose or misrepresent the individuals whose data they are using? This links directly back to the GDPR discussion in Palmer's article. GDPR's focus on consent, data minimization, and user control can be read as legal efforts to institutionalize some of the values that ethics of care prioritize. Instead of presuming data can be used simply because it's public, GDPR mandates that individuals be notified, respected, and given a voice in how their information is managed. Buchanan's work illustrates how easily those ethical considerations get ignored in data-rich settings, and the ethics of care helps highlight why that oversight matters. It's not merely a matter of obeying regulations, but a matter of acknowledging and respecting the human footprint behind each data point. The U.S. current approach to data privacy (fragmented, reactive, and driven by economic rather than ethical considerations) does not express the values that Buchanan or ethics of care encourage. Without clear and consistent standards like those found in GDPR, U.S. organizations are under no obligation to foresee harm, be empathetic, or think about the long-term effects of their data utilization on people. Ethics of care would argue that such disregard is not just irresponsible but morally wrong, especially in light of the asymmetry of power between the data collectors and the common users.

In addition, Buchanan states that ethical review boards and oversight mechanisms struggle to keep up with technological advancements. Ethics of care embraces the notion that ethical frameworks need to develop in tandem with technology and that moral responsibility need not be outsourced or postponed. Rather, it needs to be built into data system design, policy writing, and organizational day-to-day practices dealing with personal data. GDPR provides such a framework, one that foregrounds not just compliance but a culture of responsibility and care. Ethics of care strongly supports this shift, arguing that any system collecting or processing human data must be driven by empathy, attentiveness to context, and respect for the dignity of the people involved. In this perspective, Buchanan's analysis also supports the case for the U.S. to implement GDPR-like privacy laws. Not only would this move fill regulatory gaps, but it would also advance a more ethical, human-centered data governance. The ethics of care teaches us that the ultimate test of a data policy is not whether it is profitable or efficient, but whether it honors, protects, and cares for the individuals it impacts.

Raneem Alarian
July 9, 2025

Conclusion

In conclusion, embracing privacy regulations such as the GDPR in the United States is not merely a technical or legal choice. It is a moral one. As both Zimmerman and Buchanan illustrate, individuals are unknowingly vulnerable when their information is gathered and utilized without explicit consent. The present legislation in the United States is not protective or transparent enough. Through the ethics of care lens, it is evident that we are morally bound to handle individuals with respect and compassion, particularly when they are placed in a vulnerable situation online. Some might state that enhanced regulations would cause inconvenience to companies or hinder innovation. Nevertheless, protecting individuals' privacy and well-being must be prioritized. Privacy is not merely a matter of information, but a matter of feeling secure, respected, and in control. If we are to restore trust between users and the businesses that manage their data, the United States must shift towards policies that echo care, accountability, and responsibility; and GDPR sets a good example of how to accomplish that.

Raneem Alarian
July 9, 2025

References

Buchanan, E. (2017). *Considering the ethics of big data research: A case of Twitter and ISIS/ISIL*. PLOS ONE, 12(12), e0187155

Palmer, D. (2018). *GDPR: An executive guide to what you need to know.* ZDNet. https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

Zimmer, M. (2010). "But the data is already public": On the ethics of research in Facebook. *Ethics and information technology, 12*(4), 313-325